Privacy Policy
Last updated: 10 June 2026

Introduction

Kep Italia S.r.l. (hereinafter also referred to as the "Company"), in its capacity as Data Controller, informs you that Regulation (EU) No. 2016/679 (the "GDPR") and the applicable privacy legislation govern the protection of Personal Data.

The Company processes Personal Data in accordance with the principles of fairness, lawfulness, transparency and necessity, as provided for by the applicable legislation.

This Privacy Notice ("Privacy Policy") describes how the Personal Data of users who use the Application and the associated services ("Service") are collected, used and protected.

To this end, pursuant to Article 13 of the GDPR, the following information is provided.

1. Data Controller

The Data Controller is Kep Italia S.r.l., with registered office at Via Alessandro Volta 11/13 – Calvagese della Riviera (BS), Tax Code and VAT No. 03418990168. Contact details: contact@kepitalia.com

2. Types of Data Processed and Methods of Processing

2.1 Personal Data Provided by the User

The User may voluntarily choose to upload Personal Data, including:

• Identification data (first name, last name, date of birth)
• Contact data (e-mail address, telephone number)
• Other information freely provided in the context of using the Service

The Processing of Personal Data may consist of collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, comparison or interconnection, restriction, erasure and destruction, pursuant to Article 4(2) GDPR.

The Processing may be carried out by electronic, IT and telematic means, adopting appropriate technical and organisational measures to ensure the security and confidentiality of the data.

2.2 Health Data (Medical Data)

The User may decide to upload, through the Application and the integrated NFC technology, data belonging to the special categories referred to in Article 9 GDPR, including:

- medical conditions;
- allergies;
- medications taken;
- previous clinical information;
- identifiable physical characteristics;
- other information useful in the event of an emergency.

Health Data uploaded through the Application are stored exclusively online and/or on the User's NFC device.

Kep Italia may exclusively access aggregated and anonymised numerical data relating to registrations made by users and, upon their request, proceed with their deletion.

Under no circumstances may Kep Italia view, consult or access Health Data or medical information entered into the APP, which remain under the User's exclusive control.

Therefore, the User remains solely responsible for the accuracy, completeness, updating and lawfulness of the information and data uploaded, entered or shared through the platform.

Health Data may be read by anyone using an NFC-compatible device, without authentication, in order to allow rapid access to vital information in the event of an emergency.

For Health Data relating to minors under 18 years of age, the upload must be carried out by a parent or legal guardian, who assumes responsibility for it.

The Data Controller shall not be liable for:

- incorrect Health Data entered by the User;
- voluntary or involuntary transfers (e.g. transfer of the device);
- use of the data by third parties following access via NFC.

2.3 Anonymous Usage Data

The Data Controller may collect anonymous and aggregated data relating to the use of the Application for statistical purposes and service improvement purposes.

Such data cannot be linked to identified or identifiable natural persons and do not fall within the scope of application of the GDPR.

2.4 Cookies and Similar Technologies

To ensure the proper functioning of the services offered and improve the user experience, the App uses certain third-party technologies comparable to cookies, such as device identifiers (Device ID), authentication tokens, statistical analysis tools and technical monitoring systems. For further information, please refer to the Cookie Policy.

3. Purposes and Legal Bases of Processing

Purpose of Processing	**Legal Basis**	**Provision of Data**
Account management and provision of the Service	Art. 6(1)(b) GDPR - Performance of a contract	Mandatory
Compliance with legal obligations	Art. 6(1)(c) GDPR - Legal obligation	Mandatory
Direct marketing and promotional communications	Art. 6(1)(a) GDPR - Data Subject's Consent	Optional
Profiling and preference analysis	Art. 6(1)(a) GDPR - Data Subject's Consent	Optional
Processing of Health Data (where voluntarily uploaded by the User)	Art. 9(2)(a) GDPR - Data Subject's Explicit Consent	Optional

The provision of data for account management and compliance with legal obligations is mandatory: failure to provide such data will make it impossible to provide the Service or comply with legal obligations.

The provision of data for marketing, profiling and the uploading of Health Data is optional: any refusal does not affect the use of the basic Service, but results in the inability to receive commercial communications, benefit from personalised content or use functionalities related to medical data.

4. Recipients of the Data

Pursuant to Article 13(1)(e) GDPR, Personal Data may be disclosed to and processed by the following categories of recipients:

• Technology service providers and software houses, for the management and maintenance of the Application;

- Commercial partners and consultants (legal, tax, administrative), within the scope of providing the Service;
- Public bodies and competent Authorities, where required by law or upon their request;
- Employees and collaborators of the Data Controller authorised to process data within the scope of their respective duties.

The list of Data Processors is available at the Company's registered office.

5. Transfer of Data to Third Countries

In the context of providing the services offered through the App, certain Personal Data may be processed by providers located outside the European Economic Area (EEA) or may involve access to data by companies belonging to international groups established in third countries, including the United States of America.

In particular, possible transfers to third countries may occur in relation to the following services:

• YouTube (Google LLC), for the display of video content integrated into the App;
• Google Analytics, for the processing of aggregated statistics concerning the use of the App;
• Google Sign-In, for user authentication through Google accounts;
• Sign in with Apple, for user authentication through Apple accounts.

Such transfers are carried out in compliance with Articles 44 et seq. of Regulation (EU) 2016/679 (GDPR) and are based, where necessary, on appropriate safeguards for the protection of Personal Data, such as the Standard Contractual Clauses (SCCs) approved by the European Commission, adequacy decisions where applicable, or other instruments provided for by the applicable legislation.

With regard to the technological infrastructure of the App and the additional providers used by the Data Controller, it is specified that no transfer of data to Third Countries takes place, since:

• the application infrastructure hosted on Amazon Web Services (AWS) is located within the European Union;
• the Sentry monitoring and diagnostic service is configured on infrastructures located within the European Union;
• the MailUp e-mail communication service, used exclusively upon the Data Subject's Consent for marketing and promotional communications purposes, is hosted on infrastructures located within the European Union.

It is understood that, should it become necessary in the future to transfer Personal Data to Third Countries other than those indicated above, the Data Controller shall adopt all measures required by the applicable legislation in order to ensure a level of protection of Personal Data substantially equivalent to that guaranteed within the European Union.

6. Data Retention

Personal Data are retained for the time necessary to provide the Service. Health Data are not stored by the Data Controller but are recorded exclusively online. Personal Data processed for marketing purposes will be processed until the Data Subject withdraws Consent.

7. Rights of the Data Subject

Where the relevant conditions are met, all rights provided for under Articles 15 et seq. GDPR may be exercised in relation to Personal Data, including specifically: a) the right of access to Personal Data (Art. 15 GDPR); b) the right to rectification where data are inaccurate (Art. 16 GDPR); c) the right to erasure of data (Art. 17 GDPR); d) the right to restriction of Processing (Art. 18 GDPR); e) the right to data portability, namely to receive the Personal Data provided in a structured, commonly used and machine-readable format

and to have them transmitted to another Data Controller without hindrance (Art. 20 GDPR); f) the right to object to Processing (Art. 21 GDPR).

In the event of a violation of these provisions, the Data Subject has the right to lodge a complaint with the competent Supervisory Authority (Art. 77 GDPR).

You may exercise your rights by sending an e-mail to contact@kepitalia.com

8. Withdrawal of Consent

For Processing activities based on Consent as the legal basis, the User may withdraw Consent at any time, without such withdrawal:

- affecting the lawfulness of Processing based on Consent before its withdrawal;
- affecting further Processing of the same data based on other legal grounds, such as contractual or legal obligations.

To withdraw Consent, you may write to contact@kepitalia.com

9. Data Security

The Data Controller adopts appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR, in order to prevent loss, misuse, unauthorised modification or disclosure of Personal Data.

Note on NFC Technology

As described in Section 2.2, Health Data uploaded through NFC technology are accessible to anyone with a compatible device, without authentication. This functionality is structurally connected to the emergency function of the device. Users are advised to carefully assess the information they choose to upload to the device and to adopt appropriate precautions, particularly where sensitive data are involved.

10. Changes to the Privacy Policy

This Policy may be updated at any time. Any changes will be communicated through appropriate channels.

11. Contact Details

For questions or requests, to exercise the rights referred to in Section 7, or to withdraw Consent, the User may write to contact@kepitalia.com